IN THE CLAIMS

Please cancel claims 6, 7, 14, 15, 17, 20, 21, 23, 26, and 31 and amend claims 1, 8, 16, 22, and 28 as follows.

1. (currently amended) An encrypted network system, comprising:

a network to transmit an encrypted packet; and

a computer to receive said encrypted packet from said network, and to perform a decryption operation thereupon to convert said encrypted packet to a decrypted packet, said computer including:

a network interface to provide electronic communication between said computer and said network,

a network driver to regulate said decryption operation;

a controller to perform said decryption operation;

a host memory to store data that is used or generated by said decryption operation, and

a bus providing electronic communication among said network interface, said network driver, said host memory and said controller, said controller asserting an interrupt prior to a complete transfer of said decrypted packet from said controller to said host memory, wherein said controller asserts an additional interrupt after completion of said decryption operation, and said network driver specifies an average latency value to said controller for use in said decryption operation.

2. (original) The encrypted network system of claim 1, wherein at least one security association (SA) is stored in said host memory.

3. (original) The encrypted network system of claim 2, wherein said network driver parses said encrypted packet, matches said encrypted packet with one of said at least one SA and instructs said network interface to transfer said encrypted packet and said one SA across said bus to said controller.

4. (original) The encrypted network system of claim 1, wherein said network interface includes a cryptography accelerator.

5. (original) The encrypted network system of claim 1, wherein said controller transfers said decrypted packet across said bus from said controller to said host memory.

6. (cancelled)

7. (cancelled).

8. (currently amended) A computing system for performing a decryption operation on an encrypted packet, comprising:

a network driver to regulate said decryption operation;

a controller to perform said decryption operation;

a host memory to store data that is used or generated by said decryption operation; and

a bus providing electronic communication among said network driver, said host memory and said controller, said decryption operation converting said encrypted packed into a decrypted packet, and said controller asserting an interrupt prior to a complete transfer of said decrypted packet from said controller to said host memory, wherein said controller asserts an additional interrupt after completion of said decryption operation and said network driver specifies an average latency value to said controller for use in said decryption operation.

9. (original) The computing system of claim 8, wherein said computer further includes a network interface to provide electronic communication between said computer and a network.

10. (original) The computing system of claim 9, wherein at least one security association (SA) is stored in said host memory.

11. (previously amended) The computing system of claim 10, wherein said network driver parses said encrypted packet, matches said encrypted packet with one of said at least one SA and instructs said controller to transfer said encrypted packet and said one SA across said bus to said controller.

12. (original) The computing system of claim 8, wherein said network interface includes a cryptography accelerator.

13. (original) The computing system of claim 8, wherein said controller transfers said decrypted packet across said bus from said controller to said host memory.

14. (cancelled)

15. (cancelled).

16. (currently amended) A method of decrypting an encrypted packet received by a computing system, comprising:

receiving said encrypted packet from a network;

issuing a decryption command to a controller;

specifying an average latency value to the controller;

determining a time for said assertion of said interrupt in response to said decryption command;

converting said encrypted packet to a decrypted packet;

transferring said decrypted packet to a host; [and]

asserting an interrupt at a time before completing said transfer of said decrypted packet to said host memory, and

asserting an additional interrupt upon completion of said transfer of said decrypted packet to said host memory.

17. (cancelled)

18. (original) The method of claim 16, wherein said step of converting said encrypted packet to said decrypted packet further includes:

parsing said encrypted packet;

matching said encrypted packet with a corresponding security association (SA) stored in said host memory; and

transferring said encrypted packet and said corresponding SA to a controller.

19. (original) The method of claim 16, wherein said step of converting said encrypted packet to said decrypted packet further includes authenticating said decrypted packet.

20. (cancelled)

21. (original) The method of claim 16, further including indicating said decrypted packet to a protocol stack after asserting said interrupt.

22. (currently amended) A program code storage device, comprising:

a machine-readable storage medium; and

machine-readable program code, stored on the machine-readable storage medium, the machine-readable program code having instructions that when executed cause the device to:

receive said encrypted packet from a network;

issue a decryption command to a controller;

specify an average latency value to the controller;

determine a time for said assertion of said interrupt in response to said decryption command;

convert said encrypted packet to a decrypted packet;

transfer said decrypted packet to a host memory; [and]

assert an interrupt at a time before completing said transfer of said decrypted packet to said host memory; and

assert an additional interrupt upon completion of said transfer of said decrypted packet to said host memory.

23. (cancelled)

24. (previously amended) The device of claim 22, wherein said instructions to convert said encrypted packet to said decrypted packet further includes instructions to:

parse said encrypted packet;

match said encrypted packet with a corresponding security association (SA) stored in said host memory; and

transfer said encrypted packet and said corresponding SA to a controller.

25. (previously amended) The device of claim 22, wherein said

instructions to convert said encrypted packet to said decrypted packet further includes instructions to authenticate said decrypted packet.

26. (cancelled)

27. (previously amended) The device of claim 22, further including instructions to indicate said decrypted packet to a protocol stack after the instruction to assert said interrupt.

28. (currently amended) A system, comprising:

a computer to receive an encrypted packet and to perform a decryption operation that converts said encrypted packet into a decrypted packet; and

a memory included in said computer, said computer asserting an interrupt prior to a complete transfer of said decrypted packet to said memory and an additional interrupt after completion of said decryption operation, wherein an average latency value is specified to said computer for use in said decryption operation.

29. (previously added) The system of claim 28, wherein at least one security association (SA) is stored in said memory.

30. (previously added) The system of claim 29, further including a network driver to parse said encrypted packet, to match said encrypted packet with one of said at least one SA, and adapted to instruct a network interface to transfer said encrypted

packet and said one SA across a bus to a controller.

31. (cancelled)